Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 3, No. 10, Oktober 2019, hlm. 9608-9613 http://j-ptiik.ub.ac.id

Implementasi Sistem Deteksi dan Mitigasi Serangan *Distributed Denial of Service* (DDoS) menggunakan SVM *Classifier* pada Arsitektur *Software-Defined Network* (SDN)

Jodi Chris Jordan Sihombing[1], Dany Primanita Kartikasari[2], Adhitya Bhawiyuga[3]

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]jchrisjordan@student.ub.ac.id, [2]dany.jalin@ub.ac.id, [3]bhawiyuga@ub.ac.id

Abstrak

Software-defined network (SDN) menyediakan arsitektur yang menjanjikan untuk jaringan masa depan dan dapat memberikan keuntungan dengan programabilitas pada *controller* untuk mengatur seluruh perilaku pada jaringan. Terlepas dari keuntungan yang dimiliki SDN, terdapat tantangan pada keamanan jaringan SDN. *Distributed Denial of Service* (DDoS) adalah salah satu serangan yang dapat menyerang komponen yang ada pada arsitektur SDN. Pada penelitian ini sistem deteksi dan mitigasi serangan DDoS dibangun untuk meminimalisir serangan DDoS pada arsitektur SDN dengan menggunakan SVM *Classifier*. SVM diterapkan pada model *machine learning* untuk mengklasifikasikan *traffic* normal dan *traffic* serangan DDoS berdasarkan fitur yang diambil dari *flow entries*. Dari hasil pengujian yang telah dilakukan sistem mampu mendeteksi serangan DDoS dengan rata-rata akurasi sebesar 96,83% dan waktu rata-rata deteksi 67,80 *ms*. Selain itu, sistem juga dapat mengurangi jumlah paket serangan DDoS yang dikirimkan ke *victim host.*

Kata kunci: *Software-defined Network, Distributed Denial of Service, Support Vector Machine, Machine Learning*

Abstract

Software-defined network (SDN) provides a promising architecture for future networks and can benefit from programmability on the controller to manage all behavior on the network. Apart from the advantages SDN has, there are challenges to SDN network security. Distributed Denial of Service (DDoS) is one of the attacks that can attack components that exist on the SDN architecture. In this study the detection and mitigation system of DDoS attacks was built to minimize DDoS attacks on SDN architecture using SVM Classifier. SVM is applied to the machine learning model to classify normal traffic and DDoS attack traffic based on features taken from flow entries. From the test results the system has been able to detect DDoS attacks with an average accuracy of 96.83% and an average detection time of 67.80 ms. In addition, the system can also reduce the number of DDoS attack packets sent to the victim host.

Keywords: *Software-defined Network, Distributed Denial of Service, Support Vector Machine, Machine Learning*

1. PENDAHULUAN

Software-Defined Network (SDN) adalah teknologi pada arsitektur jaringan yang memudahkan manajemen perangkat yang ada pada suatu jaringan. Dalam jaringan konvensional, *router* menerapkan semua algoritma *routing* dan memutuskan bagaimana proses *forwarding* suatu paket. Pada arsitektur SDN, fungsi *routing* dan fungsi *forwarding* dipisahkan. Arsitektur SDN menerapkan suatu konsep manajemen jaringan yang memisahkan antara *control plane* dengan *data plane*. Pada *control plane* terdapat *controller* yang bertugas mengatur bagaimana proses yang akan dilakukan terhadap suatu paket atau *traffic* jaringan yang masuk. Sedangkan *data plane* (*switch*) memiliki fungsi untuk melakukan *forwarding* paket sesuai instruksi dari *controller* (Kim, 2013).

Terlepas dari beberapa keunggulan yang dimiliki SDN seperti penyederhanaan dan fleksibilitas jaringan, terdapat tantangan penting yang patut dipertimbangkan. Salah satu

tantangan besar yang dapat menyerang keamanan pada arsitektur SDN adalah serangan *Distributed Denial of Service* (DDoS). DDoS adalah serangan terdistribusi yang bertujuan untuk menghabiskan *bandwidth* atau ketersediaan sumber daya korban dengan membanjiri server, tautan jaringan, dan perangkat jaringan dengan *traffic* yang tidak sah (Yadav, 2014). Menurut data dari *netscout*, pada paruh kedua di tahun 2018 terdapat peningkatan serangan DDoS sebesar 19 persen di seluruh dunia (Netscout, 2018). Arsitektur SDN memiliki beberapa titik yang dapat dijadikan obyek serangan DDoS, seperti *controller* SDN, infrastruktur virtual, dan *OpenFlow switch*. Setiap kali paket baru tiba di jaringan SDN dan *switch* tidak dapat menemukan *flow entries* yang cocok, paket tersebut akan diarahkan *controller* untuk diproses. Dalam kasus ini, penyerang dapat mengirimkan paket dalam jumlah besar ke dalam jaringan SDN sehingga *controller* harus memroses dan menghasilkan *flow entries* yang sesuai untuk setiap paket palsu. *Flow entries* tersebut akan memenuhi *flow table* dan menyebabkan pengguna yang sah tidak dapat mengakses suatu layanan pada jaringan (Macedo, 2016).

Berdasarkan uraian permasalahan tersebut, maka dilakukan penelitian untuk mengimplementasikan sistem yang dapat melakukan deteksi dan mitigasi serangan DDoS pada arsitektur SDN. Dalam penelitian ini, data *traffic* normal dan *traffic* serangan akan dikumpulkan dari *flow entries*. Beberapa fitur yang digunakan untuk mengklasifikasikan *traffic* jaringan yaitu standar deviasi *flow* paket, standar deviasi *flow byte*, jumlah IP *source* per interval, jumlah *flow entries* per interval, dan rasio pair *flow entries*. Data tersebut digabungkan menjadi *dataset* yang digunakan oleh *machine learning* untuk melatih model dengan algoritme SVM. Kemudian sistem deteksi dan mitigasi serangan DDoS akan melakukan pendeteksian serangan DDoS dengan mengklasifikasikan *traffic* jaringan menggunakan SVM model dan melakukan mitigasi ketika serangan DDoS terdeteksi dengan menambahkan *flow rules* pada *OpenFlow switch*.

2. KAJIAN PUSTAKA

Penelitian terdahulu yang terkait dengan serangan *Distributed Denial of Service* pada *Software-Defined Networking* (SDN) menjadi referensi dari penelitian ini. Beberapa penelitian terkait dilakukan oleh Braga, et al. (2010). Dalam penelitian tersebut, *machine learning* berbasis algoritma *Self Organizing Maps* (SOM) digunakan untuk mendeteksi serangan DDoS dengan mengekstraksi *flow statistic* pada *Openflow switch* yang memiliki korelasi dengan serangan DDoS. Metode tersebut menghasilkan akurasi deteksi yang tinggi dan waktu yang dibutuhkan untuk mendeteksi sangat cepat. Namun dalam penelitian tersebut tidak terdapat mekanisme penanganan atau mitigasi serangan DDoS dan fitur yang digunakan harus dikembangkan.

Penelitian yang dilakukan oleh Alshamrani, et al. (2017) menemukan kerentanan yang ada pada mekanisme komunikasi di dalam arsitektur SDN. Celah keamanan tersebut adalah *Misbehaviour attack* dan *NewFlow attack*. Kedua celah keamanan tersebut dapat di eksploitasi untuk membanjiri *traffic* di seluruh komponen SDN. Berdasarkan hal itu peneliti merancang sistem untuk melakukan deteksi terhadap ancaman *Misbehaviour attack* dan *NewFlow* attack menggunakan *machine learning*. Kemudian dilakukan mitigasi serangan dengan meneruskan *traffic* yang dikirim oleh penyerang ke dalam *honeypot* agar perilaku dan pola dari serangan tersebut dapat di analisis.

Dayal N, dan Srivastava S. (2017) melakukan penelitian terkait mengenai perilaku serangan DDoS pada SDN. Dalam penelitian tersebut serangan DDoS dilakukan untuk mengetahui dampak terhadap komponen jaringan SDN. Serangan tersebut dilakukan dengan beberapa jenis DDoS. Dari penelitian tersebut didapatkan parameter yang dapat digunakan untuk mendeteksi serangan DDoS anatara lain entropi alamat IP sumber, alamat IP tujuan dan jenis protokol.

3. DISTRIBUTED DENIAL OF SERVICE

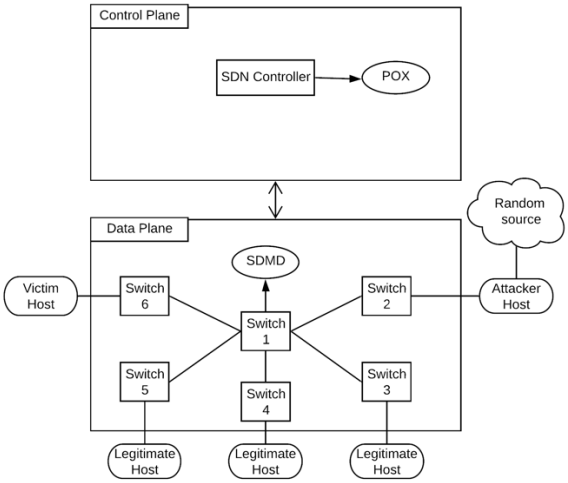
Serangan Distributed Denial of Service (DDoS) adalah suatu serangan yang dilakukan untuk menghabiskan sumber daya komputer atau jaringan komputer dengan mengirimkan lalu lintas (*traffic*) yang padat. Serangan DDoS dimulai dari penyerang yang mendistribusikan serangan dengan menggunakan mesin yang berbeda (Mousavi, 2014). Pada saat serangan, seluruh lalu lintas (*traffic*) diarahkan ke komputer korban untuk menghabiskan sumber daya (*resource*) korban. Serangan DDoS akan sering menggunakan IP *spoofing* dengan tujuan

membanjiri target dengan *traffic* yang tinggi sambil menutupi identitas sumber aslinya untuk mencegah upaya mitigasi. Jika alamat IP sumber dipalsukan dan terus diacak, upaya untuk memblokir serangan akan menjadi sulit. IP *spoofing* juga dapat mempersulit penegakan hukum dan tim keamanan siber untuk melacak pelaku serangan. Menurut Kumarasamy (2012), terdapat beberapa jenis serangan DDoS antara lain:

1. TCP SYN *Flooding* : Merupakan jenis serangan yang mengeksploitasi mekanisme 3 *way handshake* pada protokol tcp. Dalam jenis serangan ini, penyerang mengirimkan *syn* paket dalam jumlah yang besar untuk membebani target.
2. UDP *Flooding* : Merupakan jenis serangan yang mengeksploitasi *service* pada protokol UDP. Dalam jenis serangan ini, penyerang memiliki daftar alamat *broadcast* yang akan dikirimi paket UDP palsu. Paket-paket ini dikirim ke *port* acak dan mengubah lokasi target yang tidak terduga.
3. Ping (ICMP) *Flooding* : Merupakan jenis serangan pada protokol ICMP. Serangan ini bertujuan untuk menghabiskan sumber daya komputer korban dengan membanjirinya melalui *request* dari ICMP *echo*, atau yang juga dikenal sebagai *ping*.

4. PERANCANGAN

Arsitektur umum merupakan gambaran korelasi antara komponen-komponen yang berkaitan dengan sistem yang akan dibangun. Gambar 1 merupakan arsitektur umum dari sistem yang akan dibangun dalam penelitian ini.



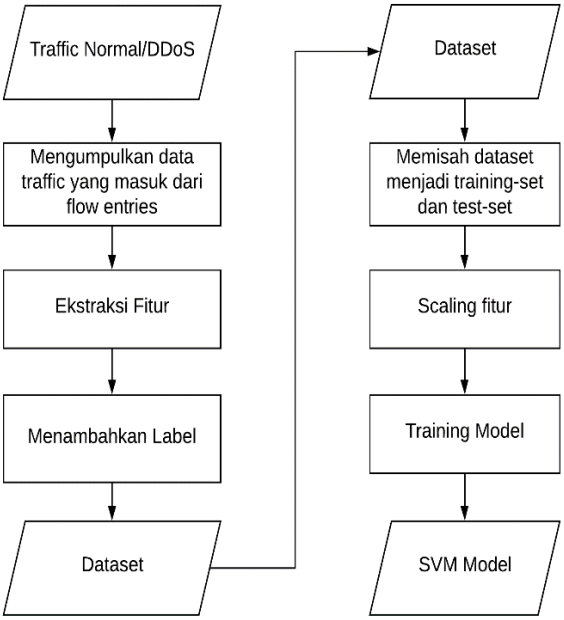
Gambar 1. Arsitektur Umum

1. *Control Plane*: Pada *Control Plane* terdapat komponen yaitu *controller* yang berfungsi sebagai otak jaringan, dimana *controller* akan bertanggung jawab atas perilaku keseluruhan jaringan seperti mekanisme *routing*, manajemen *flow*, mengatur prioritas paket, dan sebagainya. Dalam penelitian ini, *controller* yang digunakan yaitu POX yang merupakan *controller* berbasis bahasa pemrograman *python*.
2. *Data Plane*: Pada *Data Plane* terdapat komponen *openflow switch*, yang terhubung dengan *controller*. *Controller* akan memberi perintah kepada *switch* dalam melakukan *forwarding*. Masing-masing *switch* akan terhubung dengan *host* yang diantaranya terdapat *host* yang akan bertindak sebagai penyerang (*Attacker Host*), *host* yang menjadi target serangan DDoS (*Victim Host*), dan *host* yang melakukan aktivitas normal (*Legitimate Host*). Sistem deteksi dan mitigasi serangan DDoS (SDMD) akan mengumpulkan informasi *flow entries* yang terdapat pada *switch* 1 untuk mengetahui jenis *traffic* yang sedang menuju ke *victim host*.
3. Sistem Deteksi dan Mitigasi serangan DDoS (SDMD): Merupakan sistem yang digunakan untuk mendeteksi serangan DDoS menggunakan SVM *classifier* dan melakukan mitigasi serangan tersebut dengan menambahkan *flow rule* pada *switch* untuk menyaring paket yang menuju ke *victim host*.
4. *Legitimate Host*: Merupakan *endpoint* pada jaringan yang akan dibangun. Setiap *host* dapat saling berkomunikasi dengan *host* lainnya. Pada penelitian ini, masing-masing *host* akan mengirimkan *traffic* normal ke *victim host*.
5. *Victim Host*: Merupakan *host* yang menjadi target serangan DDoS, seluruh *traffic* akan ditujukan pada *victim host*.
6. *Attacker Host*: Merupakan *host* yang akan mengirimkan *traffic* serangan DDoS kepada *victim host*. Serangan DDoS tersebut akan dihasilkan dengan *tools hping3*.

4.1. Perancangan *machine learning* SVM

Untuk dapat melakukan klasifikasi *traffic* jaringan, *machine learning* harus memiliki data latih yang digunakan sebagai pembelajaran model yang akan dibuat. Data latih dihasilkan dengan mengumpulkan *traffic* pada jaringan yang akan dibangun. Pada tahap ini terdapat rancangan *traffic* jaringan yang digunakan untuk

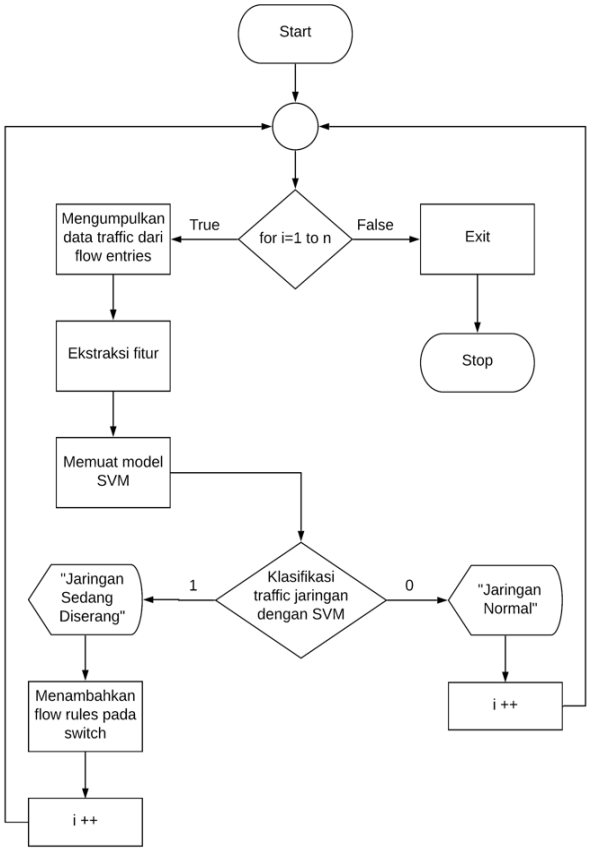
menentukan jenis *traffic* yang dikirimkan menuju ke *victim host*. Dalam penelitian ini terdapat 2 kategori *traffic* yaitu *traffic* normal dan *traffic* serangan DDoS. Seperti yang telah dijelaskan pada bagian sebelumnya, akan dilakukan pengumpulan data untuk mendapatkan data latih dari *traffic* normal dan *traffic* serangan DDoS. Setelah itu akan dihasilkan dataset yang berisi data dari *traffic* jaringan yang telah di ekstraksi. Gambar 2 merupakan perancangan *machine learning* yang dilakukan untuk membuat model SVM.



Gambar 2. Perancangan *machine learning* SVM

4.2. Perancangan Sistem Deteksi dan Mitigasi Serangan DDoS

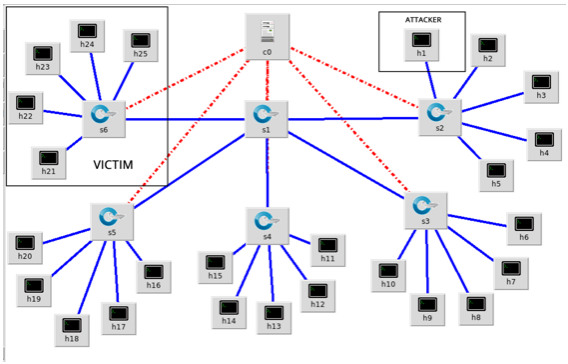
Untuk melakukan deteksi dan mitigasi serangan DDoS, terdapat beberapa langkah yang dilakukan. Langkah pertama yang dilakukan yaitu mengumpulkan data *traffic* jaringan dari *flow entries* pada *switch* yang di monitor. Kemudian diambil beberapa data yang dijadikan sebagai fitur untuk merepresentasikan kategori *traffic* tersebut. Selanjutnya akan dilakukan ekstraksi fitur untuk mendapatkan nilai pada masing-masing fitur yang akan diklasifikasikan. Fitur-fitur tersebut kemudian yang akan di proses oleh model SVM untuk memprediksi apakah itu termasuk kategori *traffic* yang normal atau *traffic* serangan DDoS. Jika fitur-fitur tersebut termasuk kategori *traffic* normal, maka sistem akan menampilkan pesan "Jaringan normal" dan kembali ke langkah awal yakni mengumpulkan data *traffic* dari *flow entries*. Sebaliknya, jika fitur-fitur tersebut termasuk kategori *traffic* serangan DDoS, maka sistem akan menampilkan pesan "Jaringan diserang" dan menambahkan *flow rules* pada *switch* untuk menyaring paket yang menuju ke *victim host*. Gambar 3 menjelaskan bagaimana langkah-langkah atau alur kerja dari sistem deteksi dan mitigasi serangan DDoS.



Gambar 3. *Flowchart* SDMD

5. PEMBAHASAN

Pengujian dilakukan menggunakan emulator jaringan *mininet* yang berjalan pada mesin virtual *ubuntu*. Mesin yang digunakan memiliki spesifikasi *memory* 8GB, dan 2,3 *GHz Intel Core i5*, 2 *processor core*. Topologi jaringan yang dibangun terdiri dari 1 *controller*, 6 *switch*, dan 25 *host*. Basis IP yang digunakan dalam jaringan ini adalah 10.0.0.0/27. Pada jaringan ini, h1 merupakan *attacker host* yang akan mengirimkan serangan DDoS menuju *victim host* yaitu seluruh *host* yang terhubung dengan s6. Kemudian *host* lainnya yang terdapat pada topologi jaringan tersebut merupakan *legitimate host*. Topologi jaringan yang digunakan dalam pengujian ini terdapat pada Gambar 4.



Gambar 4. Topologi Jaringan

Pengujian fungsionalitas dilakukan untuk mengetahui bahwa kebutuhan fungsional sistem telah terpenuhi dan berjalan sesuai dengan spesifikasi yang telah didefinisikan pada bab analisis dan perancangan sistem. Tabel 1 merupakan hasil pengujian fungsionalitas sistem.

Tabel 1. Pengujian Fungsionalitas Sistem

Pengujian	Hasil
Pengambilan data pada *flow entries*	valid
Ekstraksi fitur	valid
Deteksi serangan DDoS	valid
Menampilkan pesan serangan	valid
Menambahkan *flow rule* pada *switch*	valid

Pengujian kecepatan deteksi dan mitigasi serangan DDoS bertujuan untuk mengukur waktu yang dibutuhkan oleh sistem dalam melakukan deteksi dan mitigasi atau menanggulangi berbagai jenis serangan DDoS. Pengujian dilakukan dengan menghitung waktu eksekusi sistem saat melakukan deteksi dan saat melakukan mitigasi apabila terjadi serangan DDoS. Tabel 2 merupakan hasil pengujian kecepatan deteksi dan mitigasi serangan DDoS

Tabel 2. Pengujian Kecepatan Deteksi dan Mitigasi Serangan DDoS

Jenis *traffic*	Rata-rata kecepatan deteksi	Rata - rata kecepatan mitigasi
Normal	48,65 *ms*	-
SYN *Flooding*	60,66 *ms*	1248 *ms*
UDP *Flooding*	68,76 *ms*	1514 *ms*
ICMP *Flooding*	73,99 *ms*	1493 *ms*
Rata – Rata kecepatan deteksi serangan DDoS	67,80 *ms*	1418.3 *ms*

Pengujian akurasi deteksi serangan DDoS bertujuan untuk mengukur akurasi sistem dalam melakukan deteksi serangan DDoS. Pada tahap ini, dilakukan beberapa jenis serangan DDoS yakni *syn flooding, udp flooding, dan icmp flooding*. Percobaan dilakukan dengan mengrimkan 3 jenis serangan tersebut, kemudian data dari serangan tersebut akan diuji akurasinya pada *machine learning* SVM. Tabel 3 merupakan hasil pengujian akurasi deteksi serangan DDoS.

Tabel 3. Pengujian akurasi deteksi serangan DDoS

Jenis serangan	Rata-rata akurasi
Syn flooding	96,08%
Udp flooding	95,66%
Icmp flooding	98,76%
Rata - rata	**96,83%**

Pengujian kinerja mitigasi serangan DDoS bertujuan untuk mengetahui kinerja dari modul mitigasi dalam melakukan penganggulangan apabila terjadi serangan. Pengujian ini dilakukan dengan merekam *traffic* yang masuk pada *victim host* menggunakan *wireshark*. Hasil pengujian kinerja mitigasi serangan DDoS dijelaskan pada Tabel 4.

Tabel 4. Pengujian kinerja mitigasi serangan DDoS

	Jumlah paket serangan pada *victim host*
SDMD Tidak Aktif	1855
SDMD Aktif	864

6. KESIMPULAN

Berdasarkan hasil dari penelitian yang telah dilakukan dapat ditarik beberapa kesimpulan, yakni:

1. Sistem deteksi dan mitigasi serangan DDoS (SDMD) menggunakan SVM *classifier* dapat diterapkan pada arsitektur SDN. SDMD melakukan deteksi serangan DDoS menggunakan *machine learning* berbasis algoritme *Support Vector Machine* (SVM). Deteksi serangan DDoS dilakukan dengan mengklasifikasikan *traffic* normal dan *traffic* serangan DDoS. Data dari *traffic* jaringan dikumpulkan dari informasi *flow entries* yang terdapat pada *flow table Openflow switch*. Beberapa fitur yang

digunakan untuk merepresentasikan *traffic* jaringan yaitu standar deviasi paket, standar deviasi *flow byte*, jumlah IP *source* per interval, jumlah *flow entries* per interval, dan rasio *pair flow entries*.

2. Mekanisme mitigasi serangan DDoS dilakukan dengan menambahkan *flow rule* pada *switch* untuk menyaring paket yang menuju ke *victim host*. Setelah *flow rule* tersebut ditambahkan pada *flow table switch*, *switch* akan melakukan *drop* pada setiap paket yang berasal dari IP *source* penyerang, tetapi setiap paket yang berasal dari IP *source legitimate host* akan diteruskan.
3. Berdasarkan pengujian yang telah dilakukan, kinerja SDMD dalam melakukan deteksi serangan DDoS sangat baik. Akurasi yang didapatkan dalam melakukan deteksi serangan DDoS adalah 96,08%, 95,66%, dan 98,76% untuk masing-masing serangan *syn flooding, udp flooding, icmp flooding*. Sistem juga dapat menanggulangi dan meminimalisir dampak dari serangan DDoS. Hal tersebut dapat dibuktikan dari jumlah paket serangan yang masuk ke *victim host* menurun ketika SDMD diaktifkan.

7. DAFTAR PUSTAKA

Alshamrani A., et al. 2017. *A Defense System for Defeating DDoS Attacks in SDN based Networks*. Session: Network Virtualization and Software-Defined Networks.

Braga, R. et al. 2010. *Lightweight DDoS flooding attack detection using NOX/OpenFlow*, in Proceedings of the 35th Annual IEEE Conference on Local Computer Networks (LCN '10), pp. 408–415.

Dayal, N., dan Srivastava S. 2018. *An RBF-PSO based approach for early detection of ddos attacks in SDN*. in International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India,January 3-7, 2018, pp. 17–24.

Macedo, R., de Castro, R., Santos, A., Ghamri-Doudane, Y., dan Nogueira,M. 2016. InGlobal Communications Conference (GLOBECOM). *Self-organized SDN controller cluster conformations against DDoS attacks effects*. IEEE, pp.1-6.

Phan T. V., dan Park M. 2019. *Efficient Distributed Denial-of-Service Attack Defense in SDN-Based Cloud*, IEEE Access, vol. 7, pp. 18701-18714.

Mahjabin, T., Xiao, Y., Sun, G. dan Jiang W., 2017. International Journal of Distributed Sensor Networks. A survey of distributed denial-of-service attack, prevention, and mitigation techniques, [online] Tersedia di: <https://www.researchgate.net/publication/321775189_A_survey_of_distributed_denial-of-service_attack_prevention_and_mitigation_techniques> [Diakses 2 Oktober 2019]

Moura, J., dan Serrao C. 2019. Information. *SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks*. 10(3): p. 106.

Yang L., Zhao H. 2018. *DDoS attack identification and defense using SDN based on machine learning method* Proc. - 2018 15th Int. Symp. Pervasive Syst. Algorithms Networks, I-SPAN, IEEE (2019), pp. 174-178.